CISO MAG

beyond cybersecurity

Volume 4 | Issue 04 | April 2020

NETWORK SECURITY POWER LIST

SHOWCASING THE POWERHOUSES IN CYBERSECURITY

CISO MAG
beyond cybersecurity

Volume 4 | Issue 4
April 2020

Image credits: Shutterstock
Illustrations, Cover design & Layouts by: Rajashakher Intha

EDITOR'S NOTE

NETWORK SECURITY IN THE TIME OF A GLOBAL PANDEMIC

The world is going through some of its toughest moments in recorded history. Lockdowns have shut down offices, transportation systems and have impacted industries like travel & tourism, food & beverages, entertainment, sports and others. Stock exchanges have plummeted and millions of daily wage workers and front line workers are temporarily out of work. With half the world's employees working remotely, from home, the global networks have been put to the ultimate test. Apart from the huge draw on bandwidth, the security of the network also gains vital importance.

Digitization and adoption of cloud technologies has extended the corporate network further out into the internet—beyond the realms of firewalls. Today, even the concept of WAN and branch office is further extended. Employees are working from home, especially under the COVID-19 situation, with social distancing becoming a norm. In the borderless network where partners, customers, suppliers, and even employees connect to the corporate network from remote locations around the globe, it is of paramount importance to take into account the security of network—both internal as well as external.

To validate the research on the usage of network security solutions, *CISO MAG* conducted a multiple-choice survey, in the month of February 2020. The results of this global survey form the basis of our research and conclusions on the state of network security. Some of the key findings of the survey were: more than 60% of organizations have adopted multiple layers of protection. Also, 80.6% of respondents suggest using an amalgamation of NAC (Network Access Control) policies. *CISO MAG* also took a Snap Poll to understand the precautions companies have taking to combat the threats looming on the cyberspace amid COVID-19, where a large chunk of the respondents (70%) stated that they were using company VPNs to securely log in to the company network. Nearly all the respondents also stated that their companies had secured the endpoint device (laptop/phone) that the employees are using at home.

This is also the first **Power List** issue of *CISO MAG* this year and this issue is dedicated to **Network Security**. This issue also features the brand stories of best network security companies, globally, put together by the *CISO MAG* editorial team.

Tell us what you think of this issue. If you have any suggestions, comments or queries, please reach us at editorial@cisomag.com.

Jay Bavisi
Editor-in-Chief

INDEX

12 | BUZZ

5 Key Cybersecurity Lessons from SecOps

20 | UNDER THE SPOTLIGHT

Companies of All Sizes Now Recognize That They Are Potential Targets

30 | INSIGHT

Improving Cyber Hygiene With Great Social Cybersecurity Engagement

40 | KNOWLEDGE HUB

Demystifying Cyber Insurance to Enable Adoption

48 | TECH TALK

Zero Trust is Over Hyped Because Vendors are Overusing it

60 | TABLE TALK

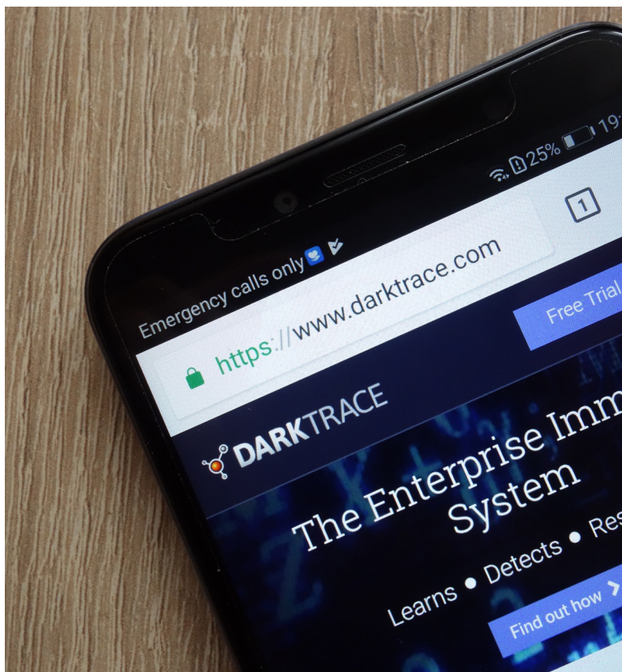
Threat Detection has Evolved from Static to Dynamic Behavioral Analysis

72 | POWER LIST

Cover Story:
Network Security - The Trends of 2020

78 | Network Security Survey

94 | Network Security Companies to Watch



CISO MAG
beyond cybersecurity

EVENTS

An **EC-Council** initiative

INTRODUCING YOU
TO THE NEXT LEVEL

VIRTUAL SERIES

events.cisomag.com

Benefits of a **Virtual Series**

Moving events online can reduce costs and carbon footprints and make attendance accessible to a wider audience.

Due to the ease of platform use and virtual location, virtual events require minimal setup time. The planning time compared to in-person events is reduced tremendously.

Viewers receive the same amount of knowledge while still sitting at home/ office

Increased Awareness and Thought-Leadership Perception for brands

Most countries are locked down currently and this is the best way to capture their head space

No geographic boundaries

For Details write to
marketing@cisomag.com

FRIEND OR FOE?

Today's cyber-attackers are masters of disguise.

Sophisticated email attacks, compromised cloud systems, vulnerable devices - it's hard to predict tomorrow's threats. AI can distinguish between legitimate activity and an emerging cyber-threat, and fight back in seconds.

DARKTRACE
World-Leading Cyber AI

CLOUD SECURITY

CISO MAG
beyond cybersecurity

POWER LIST

SHOWCASING THE POWERHOUSES IN CYBERSECURITY

Cloud Security Companies To Watch Out in **2020**

For Advertising Opportunities write to

marketing@cisomag.com

10,000 Global CISOs Will See Your Brand In The **Cloud Security Power List**

5 KEY CYBERSECURITY LESSONS FROM SECOPS

Chris Triolo, Vice President of Customer Success, Respond Software

Security Operations (SecOps) team members have interesting stories to tell about their run-ins with cyber adversaries. Some of these professionals have built and run Security Operations Centers (SOCs) for some of the world's largest companies. They've seen daily incidents that they strive to address and resolve. And from these war stories comes a fundamental understanding of some of the best practices to fight cyber criminals.

BUZZ....

1. Pay attention to lateral attacks

The steady flow of news articles about vulnerabilities in IoT devices may seem like hyperbole, but the reality is that the risk continues to grow. In fact, during a recent proof-of-concept I worked on, an organization detected evidence of lateral movement from an IoT device (in this case, a network of security cameras) to other systems in the environment. Lateral movement is a technique where an attacker breaks into one system and uses that as a beachhead to move on to other systems in the environment. In this case, their physical security camera systems were on the same network as systems managing critical data. A best practice is to monitor all devices on the network and ensure appropriate network segmentation, so that critical systems would never be on the same network as IoT devices like security cameras and smart TVs.

2. Don't make assumptions when you tune

Another company I spoke with recently found a Zeus infection within their network. Infected internal systems were reaching out to known malicious IPs. The company had seen so many of these alerts that they assumed they were false positives and began disabling the intrusion detection signatures – that is, tuning down the sensors. Eventually they found evidence that these "false positives" were real, re-enabled the signatures, and took action to clean up the infected systems.

3. Infected systems need cleaning

It's a common occurrence for systems to be infected with malware and "beacon out" – that is, they're communicating with attacker systems outside the network. In some cases, the customer who has already anticipated this situation, has technology controls in place that drop or block the traffic on its way out of the network so that the internal system can't reach out to the external system of the attackers. Some organizations will say, "No problem! The traffic is blocked, I'm safe." However, that still leaves them with a compromised or infected system inside the network that needs be cleaned. Just because the malicious traffic is blocked, doesn't mean it can be ignored. What if the system is a laptop and is taken home (out of the office) where it's no longer protected? There's nothing to stop it from communicating with the attacker's system when on the employee's home Wi-Fi.